DETECTION OF DUPLICATE CLIENT IDENTITIES IN A COMMUNICATION SYSTEM

ABSTRACT OF THE DISCLOSURE

A system for detecting clones in a communication network. The system of this invention includes a KDC (key distribution center), coupled to clients and application servers through the communication network. When a client wishes to access an application server, it contacts the KDC. The KDC then verifies whether the client is authorized to access the application server. In one aspect, this verification is done by performing an authenticated Diffie-Hellman key exchange. After the client is authenticated by the KDC, it issues a ticket containing a session key. In one aspect, this ticket is valid for a designated duration. In another aspect, the KDC simply records when the ticket was issued. After the ticket is issued, the session key is used by the client for authenticating its access request and accessing the application server. A clone wishing to access the application server, needs to contact the KDC to perform its own authenticated key agreement, to obtain a ticket with a new random session key. The clone having duplicated the identity of the client, now contacts the KDC to request access to the application server. The KDC then checks whether the access request is prior to expiration of the ticket previously issued to the authorized client. If so, the access request is flagged as a possible fraudulent request. In this manner, the present invention grants access to authorized clients while preventing access to unauthorized clients. Note that cloning detection may take place at the KDC. Or, it may occur at the application server to which access is being sought.